MORPHO

SECURITY TARGET LITE FOR IDEAL PASS V2 BAC APPLICATION

Contract no.: N/A

Reference: 2014_0000001657

Table of contents

Table of figures

Introduction

1.1 Security Target and TOE reference

ST reference :

Title	:	MACHINE Readable Travel Document – Basic Access Control – CC IDeal Pass V2
Version	:	5.0.0
Security target identifier	:	2014_0000001657

TOE reference :

Chip identifier	:	M7892 B11
Masked chip reference	:	IDealPass_v2N_M7892_1_0_0
Crypto library		Toolbox v1.02.013
Chip Component Assurance Level		EAL6+, augmented with ALC_FLR.1
TOE Identifier		IDEALPASSV2SAC/EAC_NTePASSPORT/1.0.0
Administration guidance	:	2013_1000001952 - Preparative Procedures
User guidance	:	2013_1000001953 - Operational User Guidance

CC compliance :

Version	:	3.1
Assurance level	:	EAL 4 augmented with ALC_DVS.2 ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3
Chip and cryptolibrary certificate reference	:	BSI-DSZ-CC-0782-2012 M7892 B11
Protection Profile		BSI-CC-PP-0055, Version 1.10 [R5]

1.2 General overview of the Target of Evaluation (TOE)

1.2.1 TOE type

The *Target of Evaluation* (TOE) is a contact/contactless chip programmed according to the *Logical Data Structure* (LDS) [R9] (i.e. the MRTD's chip) and providing the advanced security methods Basic Access Control (BAC) as defined in the Technical reports of "ICAO Doc 9303" [R9]. The MRTD's chip allows the authenticity of the *travel document* and the identity of its holder to be checked during a border control, with the support of an inspection system.

The MRTD's chips are intended to be inserted into the cover page of traditional passport booklets. They can be integrated into modules, inlay or datapage. The final product can be a passport, a plastic card etc…

The Chip Authentication prevents data traces described in [R9] informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps:

- the inspection system communicates by means of secure messaging established by Basic Access Control,
- the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object,
- the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive and
- the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE and the TOE environment.

1.2.2 Usage and major security features of the TOE

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this protection profile contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the TOE description MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this Security Target the MRTD is viewed as unit of

(a) the physical MRTD as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder

(1) the biographical data on the biographical data page of the passport book,

(2) the printed data in the Machine-Readable Zone (MRZ) and

(3) the printed portrait.

(b) the logical MRTD as data of the MRTD holder stored according to the Logical Data Structure [6] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder

(1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(2) the digitized portraits (EF.DG2),

(3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both

(4) the other data according to LDS (EF.DG5 to EF.DG16) and

(5) the Document security object.

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [6]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitive biometrics as optional security measure in the 'ICAO Doc 9303' [6]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This Security Target addresses the protection of the logical MRTD (i) in integrity by writeonly-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This Security Target addresses the Active Authentication.

The Basic Access Control is a security feature which is mandatory supported by the TOE. The inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the

logical MRTD by means of private communication(secure messaging) with this inspection system [R9], normative appendix 5.

1.2.3 TOE life cycle

The product's life cycle is organised as follows:

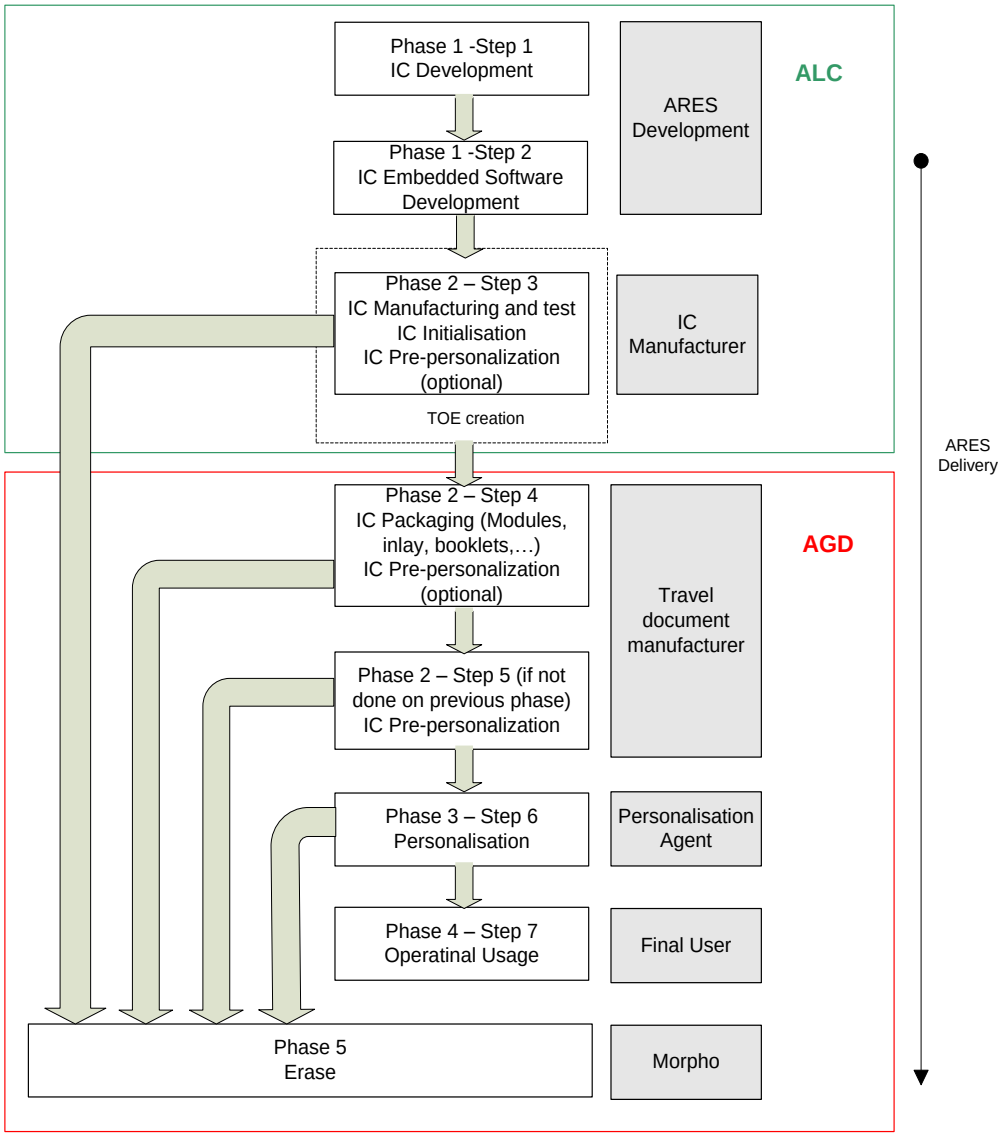


Figure 1 : TOE life cycle

Phase number	Phase name	Description / Authority
1	Development	(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components. Actor : Morpho and Infineon (Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components. The Morpho ePassport code is securely delivered directly from the software developer (Morpho.) to the IC manufacturer (Infineon). Actors : Morpho and Infineon
2	Manufacturing	(Step3) In a first step the TOE integrated circuit is produced containing the MRTD's chip Dedicated Software and the parts of the MRTD's chip Embedded Software. The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The ePassport application code will be integrated in the FLASH memory by the IC manufacturer. Actors : Infineon (Step 4) is performed by the Personalization Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), (iii) the Document security object. The signing of the Document security object by the Document Signer [R9] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use. This Security Target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [R9]. This approach allows but does not enforce the separation of these roles. Actor : Morpho

Phase number	Phase name	Description / Authority
3	Personalization agent	(Step6) The personalization of the MRTD includes (i) the survey of the MRTD holder's biographical data, (ii) the enrolment of the MRTD holder biometric reference data (i.e. the digitized portraits and the optional biometric reference data), (iii) the printing of the visual readable data onto the physical MRTD, (iv) (iv) the writing of the TOE User Data and TSF Data into the logical MRTD and (v) configuration of the TSF if necessary. Actor : issuing State or Organization
4	Operational Use	(Step 7) The TOE is used as MRTD's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the Issuing State or Organization and can be used according to the security policy of the Issuing State but they can never be modified Actor : Passport Holder
5	Erase	The erase function is included into the TOE. The access to this function is granted only and only if Mutal Authentication with Key set n°1 is successful. After the erase all TOE data (Sensitive and non sensitive) are Erased. Infineon Bootloader will be re-activated. The erase function is not accessible after Phase 3 (Operational Usage)

2 Conformance claims

2.1 Conformance with the Common Criteria

This Security Target claims conformance to:

- Part 1 of the Common Criteria, Version 3.1, Release 4 (see [R1])
- Part 2 of the Common Criteria, Version 3.1, Release 4 (see [R2]),
- Part 3 of the Common Criteria, Version 3.1, Release 4 (see [R3]),

as follows

- Part 2 extended,
- Part 3 conformant.

2.2 Conformance with an assurance package

The level of assurance targeted by this Security Target is EAL4, augmented by the following component defined in CC part 3 [R3]:

- ADV_FSP.5,
- ADV_INT.2,
- ADV_TDS.4,
- ALC_CMS.5,
- ALC_DVS.2,
- ALC_TAT.2,
- ATE_DPT.3

2.3 Conformance with a protection profile

2.3.1 Protection Profile reference

This Security Target claims strict conformance to the Protection Profile MRTD BAC [R5].

2.3.2 Protection Profile Claims rationale

The TOE type defined in this security target is exactly the same than the one defined in the PP MRTD BAC [R5]: an contact/contactless chip with embedded software, and the MRTD application conformant to ICAO [R9].

In the following, the statements of the security problem definition, the security objectives, and the security requirements are identical to those of the PP MRTD BAC [R5].

There are additions augmentations performed in this security target compare to the PP [R5].This augmentations are describ in the chapter 2.2 .All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness has been argued in the rationale sections of the present document.

2.4 Conformance with the CC supporting documents

This security target address a smartcard TOE and therefore, the associated evaluation shall be performed in compliance with all CC mandatory supporting documents related to smartcard evaluations:

2.4.1 Application of Attack Potential to Smartcards

This document [R11] shall be used instead of the CEM [R4] when calculating the attack potential of the successful attack performed during AVA_VAN analysis. This document impacts only the vulnerability analysis performed by the ITSEF, and is not detailed here.

2.4.2 Composite product evaluation for Smartcards and similar devices

This document [R12] shall be used in addition to the CC part 3 [R3] and to the CEM [R4]. This document specifies the additional information to be provided by a developer, and the additional checks to be performed by the ITSEF when performing a "composite evaluation". This is the case for the current TOE as the underlying IC M7892 B11 is already evaluated and certified under the reference : 2009/28. Therefore, the following additional assurance requirements apply for this TOE:

- ASE_COMP.1 for the security target ;
- ALC_COMP.1 for the life cycle support ;
- ADV_COMP.1 for the development activity ;
- ATE_COMP.1 for the tests activity ;
- AVA_COMP.1 for the vulnerability assessment.

The "Statement of compatibility" required by ASE_COMP additional requirements can be found in this security target, chapter 9.

3 Security problem definition

3.1 Assets

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object EF.SOD according to LDS [R9]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Due to interoperability reasons as the "ICAO Doc 9303" [R9] the TOE described in this security target specifies only the BAC mechanisms with resistance against enhanced basic attack potential granting access to

- Logical MRTD standard User Data (i.e. Personal Data) of the MRTD holder (EF.DG1, EF.DG2, EF.DG5 to EF.DG13, EF.DG16),
- Chip Authentication Public Key in EF.DG14,
- Active Authentication Public Key in EF.DG15,
- Document Security Object (SOD) in EF.SOD,
- Common data in EF.COM. The TOE prevents read access to sensitive User Data
- Sensitive biometric reference data (EF.DG3, EF.DG4).

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD holder is used by the traveler to prove his possession of a genuine MRTD.

3.2 Users / Subjects

The following individuals and IT systems have access to the TOE:

Manufacturer

"Manufacturer" is the generic term for the IC Manufacturer producing the integrated circuit as well as for the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of the TOE during the Phase 2 Manufacturing (step 3 to step 5). In this Security Target, the TOE does not distinguish between the users "IC Manufacturer" and the "MRTD Manufacturer" using this role Manufacturer.

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by:

establishing the identity of the holder for the biographic data in the MRTD,

enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s),

writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability,

writing the initial TSF data and

signing the Document Security Object defined in [R9].

Terminal

A terminal is any technical system communicating with the TOE through its contactless interface.

Inspection system (IS)

A technical system used by the border control officer of the receiving State:

examining an MRTD presented by the traveler and verifying its authenticity,

verifying the traveler as the MRTD holder.

The **Basic Inspection System** (BIS):

contains a terminal for the contactless communication with the MRTD's chip,

implements the terminals part of the Basic Access Control Mechanism,

gets the authorization to read the logical MRTD under the Basic Access Control by optically reading the MRTD or other parts of the passport book providing this information.

The **General Inspection System** (GIS) is a Basic Inspection System which implements additionally the Chip Authentication Mechanism.

The **Extended Inspection System** (EIS) in addition to the General Inspection System:

implements the Terminal Authentication Protocol,

is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data. The security attributes of the EIS are defined by the Inspection System Certificates

Application note:

This security target does not distinguish between the BIS, GIS and EIS because the Chip Authentication Mechanism and the Extended Access Control is outside the scope.

MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

Attacker

A threat agent trying:

- to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the printed MRZ data),
- to read or to manipulate the logical MRTD without authorization, or
- to forge a genuine MRTD.

Application note:

An impostor is attacking the inspection system as TOE IT environment independent on using a genuine, counterfeit or forged MRTD. Therefore the impostor may use results of successful attacks against the TOE but the attack itself is not relevant for the TOE.

3.3 Threats

T.Chip_ID

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. The attacker cannot read and does not know the MRZ data printed on the MRTD data page in advance. The targetted asset is the Anonymity of user.

T.Skimming

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker cannot read and does not know the MRZ data printed on the MRTD data page in advance. The targetted asset is the confidentiality of logical MRTD data.

T. Eavesdropping

An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

Note in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system.

The targetted asset is confidentiality of logical MRTD data.

T.Forgery

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data.

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

The targetted asset is the authenticity of logical MRTD data.

T.Abuse-Func

An attacker may use functions of the TOE which shall not be used in "TOE operational Use" phase in order

- to manipulate User Data,
- to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
- to disclose or to manipulate TSF Data.

This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder.

The targetted asset is confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

T.Information_Leakage

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Diffe-

rential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

The targetted asset is confidentiality of logical MRTD and TSF data.

T.Phys-Tamper

An attacker may perform physical probing of the MRTD's chip in order

to disclose TSF Data, or

to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to

modify security features or functions of the MRTD's chip,

modify security functions of the MRTD's chip Embedded Software,

modify User Data or,

to modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a prerequisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

The targetted asset is confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Malfunction

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

deactivate or modify security features or functions of the TOE or

circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation.

The targetted asset is confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.

3.4 Organisational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

P.Manufact

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.Personalization

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.

P.Personal_Data

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [R9].

Application note:

The organizational security policy P.Personal_Data is drawn from the ICAO "ICAO Doc 9303" [R9]. Note that the Document Basic Access Key is defined by the TOE environment and loaded to the TOE by the Personalization Agent

3.5 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

A.MRTD_Manufact

It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

Procedures shall ensure protection of TOE material/information under delivery and storage.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

A.Pers_Agent

The Personalization Agent ensures the correctness of

the logical MRTD with respect to the MRTD holder,

the Document Basic Access Keys,

the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip,

the Document Signer Public Key Certificate (if stored on the MRTD's chip).

The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys

The Inspection System is used by the border control officer of the receiving State

Examining an MRTD presented by the traveler and verifying its authenticity and

verifying the traveler as MRTD holder.

The Basic Inspection System for global interoperability

includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organization, and

implements the terminal part of the Basic Access Control [R9].

The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.

Application note:

According to [R9] the support of the Passive Authentication mechanism is mandatory whereas the Basic Access Control is optional. This ST does not address Primary Inspection Systems therefore the BAC is mandatory within this ST.

A.BAC-Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the "ICAO Doc 9303" [R9], the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to with-

stand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Application note:

When assessing the MRZ data resp. the BAC keys entropy potential dependencies between these data (especially single items of the MRZ) have to be considered and taken into account. E.g. there might be a direct dependency between the Document Number when chosen consecutively and the issuing date.

4 Security Objectives

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

OT.AC_Pers

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [R9] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

Application note:

The OT.AC_Pers implies that

the data of the LDS groups written during personalization for MRTD holder (at least EF.DG1 and EF.DG2) can not be changed by write access after personalization,

the Personalization Agents may:

add (fill) data into the LDS data groups not written yet, and

update and sign the Document Security Object accordingly. The support for adding data in the "Operational Use" phase is optional.

OT.Data_Int

The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection system is able to detect any modification of the transmitted logical MRTD data.

OT. Data_Conf

The TOE must ensure the confidentiality of the logical MRTD data groups EF.DG1 to EF.DG16. Read access to EF.DG1 to EF.DG16 is granted to terminals successfully authenticated as Personalization Agent. Read access to EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 is granted to terminals successfully authenticated as Basic Inspection System. The Basic Inspection System shall authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the Basic Inspection System.

Application note:

The traveler grants the authorization for reading the personal data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 to the inspection system by presenting the MRTD. The MRTD's chip shall provide read access to these data for terminals successfully authenticated by means of the Basic Access Control based on knowledge of the Document Basic Access Keys. The security objective OT.Data_Conf requires the TOE to ensure the strength of the security function Basic Access Control Authentication. The Document Basic Access Keys are derived from the MRZ data defined by the TOE environment and are loaded into the TOE by the Personalization Agent. Therefore the sufficient quality of these keys has to result from the MRZ data's entropy. Any attack based on decision of the "ICAO Doc 9303" [R9] that the inspection system derives Document Basic Access is ensured by OE.BAC-Keys. Note that the authorization for reading the biometric data in EF.DG3 and EF.DG4 is only granted after successful Enhanced Access Control not covered by this security target. Thus the read access must be prevented even in case of a successful BAC Authentication.

OT.Identification

The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 "Manufacturing" and Phase 3 "Personalization of the MRTD". The storage of the Pre-Personalization data includes writing of the Personalization Agent Authentication key(s).). In Phase 4 "Operational Use" the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

Application note:

The TOE security objective OT.Identification addresses security features of the TOE to support the life cycle security in the manufacturing and personalization phases. The IC Identification Data are used for TOE identification in Phase 2 "Manufacturing" and for traceability and/or to secure shipment of the TOE from Phase 2 "Manufacturing" into the Phase 3 "Personalization of the MRTD". The OT.Identification addresses security features of the TOE to be used by the TOE manufacturing. In the Phase 4 "Operational Use" the TOE is identified by the Document Number as part of the printed and digital MRZ. The OT.Identification forbids the output of any other IC (e.g. integrated circuit card serial number ICCSN) or MRTD identifier through the contactless interface before successful authentication as Basic Inspection System or as Personalization Agent.

The following TOE security objectives address the protection provided by the MRTD's chip independent of the TOE environment.

OT.Prot_Abuse-Func

After delivery of the TOE to the MRTD Holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to

disclose critical User Data,

manipulate critical User Data of the IC Embedded Software,

manipulate Soft-coded IC Embedded Software or

bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak

The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines and

by forcing a malfunction of the TOE and/or

by a physical manipulation of the TOE.

Application note:

This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker. Details correspond to an analysis of attack scenarios which is not given here.

OT.Prot_Phys-Tamper

The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with enhanced basic attack potential by means of

measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or

measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

manipulation of the hardware and its security features, as well as

controlled manipulation of memory contents (User Data, TSF Data)

with a prior

reverse-engineering to understand the design and its properties and functions.

OT.Prot_Malfunction

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

Application note:

A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective OT.Prot_Phys-Tamper) provided that detailed knowledge about the TOE's internals.

OT.Chip_Auth_Proof

The TOE must support the Basic and General Inspection Systems, to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [R9]. The authenticity prove provided by MRTD's chip shall be protected against attacks with high attack potential.

4.2 Security objectives for the Operational Environment

OE.MRTD_Manufact

Appropriate functionality testing of the TOE shall be used in step 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.MRTD_ Delivery

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non-conformance to this process.

Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.

OE.Personalization

The issuing State or Organization

- establish the correct identity of the holder and create biographical data for the MRTD,
- enroll the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and
- personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign

The issuing State or Organization must

generate a cryptographic secure Country Signing CA Key Pair,

ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and

distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.

The issuing State or Organization must

generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys,

sign Document Security Objects of genuine MRTD in a secure operational environment only and

distribute the Certificate of the Document Signer Public Key to receiving States and Organizations.

The digital signature in the Document Security Object EF.SOD relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [R9].

OE.BAC-Keys

The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the "ICAO Doc 9303" [R9] the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Basic Access Keys from the printed MRZ data with enhanced basic attack potential.

OE.Exam_MRTD

The inspection system of the receiving State or Organization must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability

includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

implements the terminal part of the Basic Access Control [R9].

OE.Passive_Auth_Verif

The border control officer of the receiving State uses the inspection system to verify the traveler as MRTD holder. The inspection systems must have successfully verified the signature of Document Security Objects and the integrity data elements of the logical MRTD before they are used. The receiving States and Organizations must manage the Country Signing CA Public Key and the Document Signer Public Key maintaining their authenticity and availability in all inspection systems.

OE.Prot_Logical_MRTD

The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The receiving State examining the logical MRTD being under Basic Access Control will use inspection systems which implement the terminal part of the Basic Access Control and use the secure messaging with fresh generated keys for the protection of the transmitted data (i.e. Basic Inspection Systems).

4.3 Security Objectives Rationale

4.3.1 Threats

T.Chip_ID The threat **T.Chip_ID** "Identification of MRTD's chip" addresses the trace of the MRTD movement by identifying remotely the MRTD's chip through the contactless communication interface. This threat is countered as described by the security objective **OT.Identification** by Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

T.Skimming The threat **T.Skimming** "Skimming digital MRZ data or the digital portrait" is countered by the security objective **OT. Data_Conf** "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys as required by the security objective for the environment **OE.BAC-Keys**.

T. Eavesdropping This threat **T. Eavesdropping** is countered by the security objective **OT. Data_Conf** "Confidentiality of personal data" through Basic Access Control using sufficiently strong derived keys.

T.Forgery The threat **T.Forgery** "Forgery of data on MRTD's chip" addresses the fraudulent alteration of the complete stored logical MRTD or any part of it. The security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD" requires the TOE to limit the write access for the logical MRTD to the trustworthy Personalization Agent (cf. OE.Personalization). The TOE will protect the integrity of the stored logical MRTD according the security objective **OT.Data_Int** "Integrity of personal data" and **OT.Prot_Phys-Tamper** "Protection against Physical Tampering". The TOE will protect the identity and authenticity of the MRTD's chip as issued by the identified issuing state or organisation by means of the chip according the security objective **OT.chip_auth_Proof**. The examination of the presented MRTD passport book according to **OE.Exam_MRTD** "Examination of the MRTD passport book" shall ensure that passport book does not contain a sensitive contactless chip which may present the complete unchanged logical MRTD. The TOE environment will detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Pass_Auth_Sign** "Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Passive_Auth_Verif** "Verification by Passive Authentication".

T.Abuse-Func The threat **T.Abuse Func** "Abuse of Functionality" addresses attacks using the MRTD's chip as production material for the MRTD and misuse of the functions for personalization in the operational state after delivery to MRTD holder to disclose or to manipulate the logical MRTD. This threat is countered by **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality". Additionally this objective is supported by the security objective for the TOE environment: **OE.Personalization** "Personalization of logical MRTD" en-

suring that the TOE security functions for the initialization and the personalization are disabled and the security functions for the operational state after delivery to MRTD holder are enabled according to the intended use of the TOE.

T.Information_Leakage The threats **T.Information_Leakage** "Information Leakage from MRTD's chip" is typical for integrated circuits like smart cards under direct attack with high attack potential.this threat is countered by the directly related security objectif **OT.Prot_Inf_Leak** "Protection against Information Leakage".

T.Phys-Tamper The threat **T.Phys-Tamper** "Physical Tampering" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objectif **OT.Prot_Phys-Tamper** "Protection against Physical Tampering".

T.Malfunction The threat **T.Malfunction** "Malfunction due to Environmental Stress" is typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against this threat is addressed by the directly related security objectif **OT.Prot_Malfunction** "Protection against Malfunctions".

4.3.2 Organisational Security Policies

P.Manufact The OSP **P.Manufact** "Manufacturing of the MRTD's chip" requires a unique identification of the IC by means of the Initialization Data and the writing of the Prepersonalization Data as being fulfilled by **OT.Identification**.

P.Personalization The OSP **P.Personalization** "Personalization of the MRTD by issuing State or Organization only" addresses the:

- the enrolment of the logical MRTD by the Personalization Agent as described in the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD", and
- the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalization of logical MRTD".

Note the manufacturer equips the TOE with the Personalization Agent Authentication key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalization Agent.

P.Personal_Data The OSP **P.Personal_Data** "Personal data protection policy" requires the TOE:

- to support the protection of the confidentiality of the logical MRTD by means of the Basic Access Control and
- enforce the access control for reading as decided by the issuing State or Organization. This policy is implemented by the security objectives **OT.Data_Int** "Integrity

of personal data" describing the unconditional protection of the integrity of the stored data and during transmission. The security objective **OT. Data_Conf** "Confidentiality of personal data" describes the protection of the confidentiality.

4.3.3 Assumptions

A.MRTD_Manufact The assumption **A.MRTD_Manufact** "MRTD manufacturing on step 4 to 6" is covered by the security objective for the TOE environment **OE.MRTD_Manufact** "Protection of the MRTD Manufacturing" that requires to use security procedures during all manufacturing steps.

A.MRTD_Delivery The assumption **A.MRTD_ Delivery** "MRTD delivery during step 4 to 6" is covered by the security objective for the TOE environment **OE.MRTD_ Delivery** "Protection of the MRTD delivery" that requires to use security procedures during delivery steps of the MRTD.

A.Pers_Agent The assumption **A.Pers_Agent** "Personalization of the MRTD's chip" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD" including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

A.Insp_Sys The examination of the MRTD passport book addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_MRTD** "Examination of the MRTD passport book". The security objectives for the TOE environment **OE.Prot_Logical_MRTD** "Protection of data from the logical MRTD" will require the Basic Inspection System to implement the Basic Access Control and to protect the logical MRTD data during the transmission and the internal handling.

A.BAC-Keys The assumption **A.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" is directly covered by the security objective for the TOE environment **OE.BAC-Keys** "Cryptographic quality of Basic Access Control Keys" ensuring the sufficient key quality to be provided by the issuing State or Organization.

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.Chip_ID	OT.Identification, OE.BAC-Keys	Section 2.3.1
T.Skimming	OE.BAC-Keys, OT. Data_Conf	Section 2.3.1
T. Eavesdropping	OT. Data_Conf	Section 2.3.1

Threats	Security Objectives	Rationale
T.Forgery	OT.AC_Pers, OT.Data_Int, OT.Prot_Phys-Tamper, OE.Pass_Auth_Sign, OE.Exam_MRTD, OE.Passive_Auth_Verif, **OT.Chip_Auth_Proof**	Section 2.3.1
T.Abuse-Func	OT.Prot_Abuse-Func, OE.Personalization	Section 2.3.1
T.Information_Leakage	OT.Prot_Inf_Leak	Section 2.3.1
T.Phys-Tamper	OT.Prot_Phys-Tamper	Section 2.3.1
T.Malfunction	OT.Prot_Malfunction	Section 2.3.1

Threats and Security Objectives - Coverage

Security Objectives	Threats	Rationale
OT.AC_Pers	T.Forgery	
OT.Data_Int	T.Forgery	
OT. Data_Conf	T.Skimming, T. Eavesdropping	
OT.Identification	T.Chip_ID	
OT.Prot_Abuse-Func	T.Abuse-Func	
OT.Prot_Inf_Leak	T.Information_Leakage	
OT.Prot_Phys-Tamper	T.Forgery, T.Phys-Tamper	
OT.Prot_Malfunction	T.Malfunction	
OT.Chip_Auth_Proof		
OE.MRTD_Manufact		
OE.MRTD_Delivery		
OE.Personalization	T.Abuse-Func	
OE.Pass_Auth_Sign	T.Forgery	
OE.BAC-Keys	T.Chip_ID, T.Skimming	
OE.Exam_MRTD	T.Forgery	
OE.Passive_Auth_Verif	T.Forgery	
OE.Prot_Logical_MRTD		

Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Manufact	OT.Identification	Section 2.3.2
P.Personalization	OT.AC_Pers, OT.Identification, OE.Personalization	Section 2.3.2
P.Personal_Data	OT.Data_Int, OT. Data_Conf	Section 2.3.2

OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies	Rationale
OT.AC_Pers	P.Personalization	
OT.Data_Int	P.Personal_Data	
OT. Data_Conf	P.Personal_Data	
OT.Identification	P.Manufact, P.Personalization	
OT.Prot_Abuse-Func		
OT.Prot_Inf_Leak		
OT.Prot_Phys-Tamper		
OT.Prot_Malfunction		
OT.Chip_Auth_Proof		
OE.MRTD_Manufact		
OE.MRTD_Delivery		
OE.Personalization	P.Personalization	
OE.Pass_Auth_Sign		
OE.BAC-Keys		
OE.Exam_MRTD		
OE.Passive_Auth_Verif		
OE.Prot_Logical_MRTD		

Security Objectives and OSPs - Coverage

Assumptions	Security objectives for the Operational Environment	Rationale
A.MRTD_Manufact	OE.MRTD_Manufact	Section 2.3.3
A.MRTD_Delivery	OE.MRTD_Delivery	Section 2.3.3
A.Pers_Agent	OE.Personalization	Section 2.3.3
A.Insp_Sys	OE.Exam_MRTD, OE.Prot_Logical_MRTD	Section 2.3.3
A.BAC-Keys	OE.BAC-Keys	Section 2.3.3

Assumptions and Security Objectives for the Operational Environment - Coverage

Security objectives for the Operational Environment	Assumptions	Rationale
OE.MRTD_Manufact	A.MRTD_Manufact	
OE.MRTD_Delivery	A.MRTD_Delivery	
OE.Personalization	A.Pers_Agent	
OE.Pass_Auth_Sign		
OE.BAC-Keys	A.BAC-Keys	
OE.Exam_MRTD	A.Insp_Sys	
OE.Passive_Auth_Verif		
OE.Prot_Logical_MRTD	A.Insp_Sys	

Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended requirements

5.1 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE a sensitive family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the *audit records*.

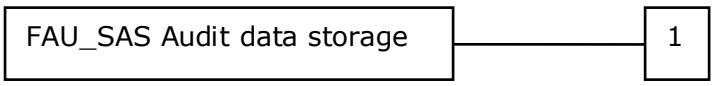
The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to store [assignment: *list of audit information*] in the audit records.

5.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

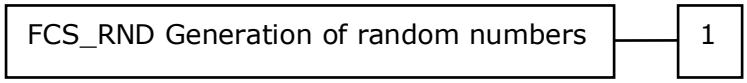
The family "Generation of random numbers (FCS_RND)" is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component leveling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers ration

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

5.3 Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because

this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

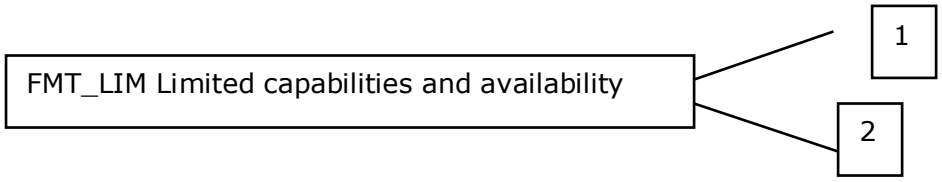
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE a sensitive family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

FMT_LIM.1 Limited capabilities.

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *Limited capability and availability policy*].

The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

FMT_LIM.2 Limited availability.

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

Application note 1: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

- the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

- the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

5.4 Definition of the Family FPT_EMS

The sensitive family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirement of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family de-

scribes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [R2].

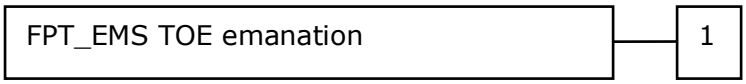
The family "TOE Emanation (FPT_EMS)" is specified as follows.

FPT_EMS TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component leveling



FPT_EMS.1	TOE emanation has two constituents:
FPT_EMS.1.1	Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
FPT_EMS.1.2	Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.
Management:	FPT_EMS.1
	There are no management activities foreseen.
Audit:	FPT_EMS.1
	There are no actions defined to be auditable.
FPT_EMS.1	TOE emanation
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].
FPT_EMS.1.2	The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security Functional Requirements

6.1 Security Functional Requirements

This section identifies the security functional requirements for the TOE. Some refinement/selection/assignment operations in the SFRs are determined in the PP MRTD BAC [R5], some are let with unspecified values. Assignments made by the PP MRTD BAC [R5] authors are marked as bold text, while assignments made by the ST author are marked as bold text and in italics. The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Document Basic Access Key Derivation Algorithm** and specified cryptographic key sizes **112 bit** that meet the following: **[**R9**], normative appendix 5**.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **Overwriting with random data** that meets the following: **none**.

Application note:

The TOE shall destroy the Triple-DES encryption key and the Retail-MAC message authentication keys for secure messaging

FCS_COP.1/SHA Cryptographic operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA224, SHA-256,SHA 384 and SHA 512** and cryptographic key sizes **none** that meet the following: **FIPS 180-2**.

Application note:

This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [R9].

FCS_COP.1/ENC Cryptographic operation

FCS_COP.1.1/ENC The TSF shall perform **secure messaging (BAC) - encryption and decryption**

in accordance with a specified cryptographic algorithm **Triple-DES CBC** and cryptographic key sizes **112 bits** that meet the following: **46-3 [R14] and [**R9**], normative appendix 5, A5.3**.

Application note:

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FCS_COP.1/AUTH Cryptographic operation

FCS_COP.1.1/AUTH The TSF shall perform **symmetric authentication - encryption and decryption**

in accordance with a specified cryptographic algorithm **Triple-DES in CBC mode** and cryptographic key sizes **112 bits** that meet the following: **FIPS 46-3 [R14]**.

Application note:

This SFR requires the TOE to implement the cryptographic primitive for authentication attempt of a terminal as Personalization Agent by means of the symmetric authentication mechanism (cf. FIA_UAU.4).

FCS_COP.1/MAC Cryptographic operation

FCS_COP.1.1/MAC The TSF shall perform **secure messaging - message authentication code**

in accordance with a specified cryptographic algorithm **Retail MAC** and cryptographic key sizes **112 bits** that meet the following: **ISO 9797 (MAC algo-**

rithm 3, block cipher DES, Sequence Message Counter, padding mode 2).

Application note:

This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by the Basic Access Control Authentication Mechanism according to the FCS_CKM.1 and FIA_UAU.4.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

(1) to read the Initialization Data in Phase 2 "Manufacturing",

(2) to read the random identifier in Phase 3 "Personalization of the MRTD",

(3) to read the random identifier in Phase 4 "Operational Use" on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note:

The IC manufacturer and the MRTD manufacturer write the Initialization Data and/or Pre-personalization Data in the audit records of the IC during the Phase 2 "Manufacturing". The audit records can be written only in the Phase 2 Manufacturing of the TOE. At this time the Manufacturer is the only user role available for the TOE. The MRTD manufacturer may create the user role Personalization Agent for transition from Phase 2 to Phase 3 "Personalization of the MRTD". The users in role Personalization Agent identify themselves by means of selecting the authentication key. After personalization in the Phase 3 (i.e. writing the digital MRZ and the Document Basic Access Keys) the user role Basic Inspection System is created by writing the Document Basic Access Keys. The Basic Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will use the Document Basic Access Key to authenticate the user as Basic Inspection System.

In the "Operational Use" phase the MRTD must not allow anybody to read the ICCSN, the MRTD identifier or any other unique identification before the user is authenticated as Basic Inspection System (cf. T.Chip_ID). Note that the terminal and the MRTD's chip use a (randomly chosen) identifier for the communication channel to allow the terminal to communicate with more then one RFID. If this identifier is randomly selected it will not violate the OT.Identification.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

(1) to read the Initialization Data in Phase 2 "Manufacturing",

(2) to read the random identifier in Phase 3 "Personalization of the MRTD",

(3) identify themselves by selection of the authentication key on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

The Basic Inspection System and the Personalization Agent authenticate themselves. The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

(1) Basic Access Control Authentication Mechanism,

(2) Authentication Mechanism based on Triple-DES.

Application note:

The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

The Basic Access Control Mechanism is a mutual device authentication mechanism defined in [R9]. In the first step the terminal authenticates itself to the MRTD's chip and the MRTD's chip authenticates to the terminal in the second step. In this second step the MRTD's chip provides the terminal with a challenge-response-pair which allows a unique identification of the MRTD's chip with some probability depending on the entropy of the Document Basic Access Keys. Therefore the TOE shall stop further communications if the terminal is not successfully authenticated in the first step of the protocol to fulfill the security objective OT.Identification and to prevent T.Chip_ID. The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2).

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

(1) Basic Access Control Authentication Mechanism,

(2) Symmetric Authentication Mechanism based on Triple-DES to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

(1) The TOE accepts the authentication attempt as Personalization Agent by the Symmetric Authentication Mechanism with the Personalization Agent Key during personalization phase of the product's life cycle (phase 3),

(2) the TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

Application note:

In case the "Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Extended Access Control" [R6] should also be fulfilled the Personalization Agent should not be authenticated by using the BAC or the symmetric authentication mechanism as they base on the two-key Triple-DES. The authentication of the personalization agent is only possible during phase 3 of the life-cycle, using symetric authentication mechanism. This can be considered as a refinement of the SFR FIA_UAU.5 of the PP. However, this refinement is more restrictive than the PP, increase the level off security and therefore, do not impact the conformity to the PP.

The Basic Access Control Mechanism includes the secure messaging for all commands exchanged after successful authentication of the inspection system. The Personalization Agent may use Symmetric Authentication Mechanism without secure messaging mechanism as well if the personalization environment prevents eavesdropping to the communication between TOE and personalization terminal. The Basic Inspection System may use the Basic Access Control Authentication Mechanism with the Document Basic Access Keys. The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **each command sent to the TOE during a BAC mechanism based communication after successful authentication of the terminal with Basic Access Control Authentication Mechanism**.

Application note:

The Basic Access Control Mechanism specified in [R9] includes the secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on Retail-MAC whether it was sent by the successfully authenticated terminal (see FCS_COP.1/MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated BAC user.

Note that in case the TOE should also fulfill [R6] the BAC communication might be followed by a Chip Authentication mechanism establishing a new secure messaging that is distinct from the BAC based communication. In this case the condition in FIA_UAU.6 above should not contradict to the option that commands are sent to the TOE that are no longer meeting the BAC communication but are protected by a more secure communication channel established after a more advanced authentication process. The TOE shall meet the requirement « Authentication failure handling (FIA_AFL.1) » as specified below (Common Criteria Part 2).

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **3** unsuccessful authentication attempts occur related to **Failure of a TDES based Authentication attempt**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **consecutively increase the reaction time of the TOE before a new authentication attempt**

FIA_API.1/AAP Authentication Proof of Identity

FIA_API.1.1/AAP The TSF shall provide a **Active Authentication Protocol according to** R9 to prove the identity of the **TOE**.

Application note:

This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in R5. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to R6. The terminal verifies by means of secure messaging whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Basic Access Control SFP** on **terminals gaining write, read and modification access to data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD**.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Basic Access Control SFP** to objects based on the following:

Subjects:

Personalization Agent,

Basic Inspection System

Terminal,

Objects:

data EF.DG1 to EF.DG16 of the logical MRTD,

Data in EF.COM,

Data in EF.SOD.

Security attributes:

Authentication status of terminals.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(1) the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,

(2) the successfully authenticated Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD and perform Active Authentication.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(1) Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,

(2) Any terminal is not allowed to read any of the EF.DG1 to EF.DG16 of the logical MRTD,

(3) The Basic Inspection System is not allowed to read the data in EF.DG3 and EF.DG4.

Application note:

The inspection system needs special authentication and authorization for read access to DG3 and DG4 not defined in this security target (cf. [R6] for details).

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the **Basic Access Control SFP** to **transmit and receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the **Basic Access Control SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

(1) Initialization,

(2) Personalization,

(3) Configuration.

Application note:

The configuration capabilities of the TOE are available during the pre-personalization (initialization) and personalization phases.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

(1) Manufacturer,

(2) Personalization Agent,

(3) Basic Inspection System.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note:

The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life cycle phases. The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow:**

(1) User Data to be disclosed or manipulated,

(2) TSF data to be disclosed or manipulated,

(3) Software to be reconstructed and

(4) Substantial information about construction of TSF to be gathered which may enable other attacks

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced **Deploying Test Features after TOE Delivery does not allow,**

(1) User Data to be disclosed or manipulated,

(2) TSF data to be disclosed or manipulated

(3) software to be reconstructed and

(4) substantial information about construction of TSF to be gathered which may enable other attacks

Application note:

The formulation of "Deploying Test Features " in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced provide an optional approach to enforce the same policy.

FMT_MTD.1/INI_ENA Management of TSF data

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to **write** the **Initialization Data and Pre-Personalization Data** to **the Manufacturer**.

FMT_MTD.1/INI_DIS Management of TSF data

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to **disable read access for users to** the **Initialization Data** to **the Personalization Agent**.

Application note:

According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by

allowing to write these data only once and

blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/KEY_WRITE Management of TSF data

FMT_MTD.1.1/KEY_WRITE The TSF shall restrict the ability to **write** the **Document Basic Access Keys**

Active Authenticate Keys to **the Personalization Agent**.

Application note:

According to P.Manufact the IC Manufacturer and the MRTD Manufacturer are the default users assumed by the TOE in the role Manufacturer during the Phase 2 "Manufacturing" but the TOE is not requested to distinguish between these users within the role Manufacturer. The TOE may restrict the ability to write the Initialization Data and the Pre-personalization Data by

allowing to write these data only once and

blocking the role Manufacturer at the end of the Phase 2. The IC Manufacturer may write the Initialization Data which includes but are not limited to the IC Identifier as required by FAU_SAS.1. The Initialization Data provides a unique identification of the IC which is used to trace the IC in the Phase 2 and 3 "personalization" but is not needed and may be misused in the Phase 4 "Operational Use". Therefore the external read access shall be blocked. The MRTD Manufacturer will write the Pre-personalization Data.

FMT_MTD.1/KEY_READ Management of TSF data

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to **read** the
(1) Document Basic Access Keys,
(2) Personalization Agent Keys,
(3) Active Authenticate Keys to **none**.

Application note:

The Personalization Agent generates, stores and ensures the correctness of the Document Basic Access Keys.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **side channel** in excess of **limits of the state of the art** enabling access to **Personalization Agent Authentication Keys and Active Authentication Private Keys** and **none**

FPT_EMS.1.2 The TSF shall ensure **any unauthorized users** are unable to use the following interface **smart card circuit contacts** to gain access to **Personalization Agent Authentication Keys** and **none**.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
(1) Exposure to out-of-range operating conditions where therefore a malfunction could occur,
(2) Failure detected by TSF according to FPT_TST.1.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

Application note:

The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE

can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here

assuming that there might be an attack at any time and

countermeasures are provided at any time.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **during initial start-up** to demonstrate the correct operation of **TSF data**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**.

Application note:

the FPT_TST.1 requirement describes requirement for the Personalization and Operational Use phases. Self-tests during the Manufacturing phase are described in the chip security target and have been evaluated during the chip evaluation.

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the Manufacturer** with the capability to store **the IC Identification Data** in the audit records.

Application note:

The Manufacturer role is the default user identity assumed by the TOE in the Phase 2 Manufacturing. The IC manufacturer and the MRTD manufacturer in the Manufacturer role write the Initialization Data and/or Pre-personalization Data as TSF Data of the TOE. The audit records are write-only-once data of the MRTD's chip (see FMT_MTD.1/INI_DIS).

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers with a reprocessing algorithmic that meet **AIS31 Class P2 quality metric**.

Application note:

This SFR requires the TOE to generate random numbers used for the authentication protocols as required by FIA_UAU.4.

FCS_COP.1/AA_SIGN Cryptographic operation

FCS_COP.1.1/AA_SIGN The TSF shall perform:

- **digital signature generation** in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes 192, **224, 256, 320, 384, 512, and** 521 **bits for ECDSA** that meet the following: **ISO15946-2 specified in [**R13**] for ECDSA in combination with SHA1, SHA224, SHA 256, SHA384 and SHA512**

- **digital signature generation** in accordance with a specified cryptographic algorithm **RSA and cryptographic key** sizes **1536**, **1792, 2048, 2560, 3072, 3584, and 4096 bits for RSA and 1536 that meet the following: ISO15946-2 specified in [**R12**] for RSA in combination with SHA1, SHA224, SHA 256, SHA384 and SHA512**

-

Application note:

This SFR requires the TOE to implement the hash function SHA-1 for the cryptographic primitive of the Basic Access Control Authentication Mechanism (see also FIA_UAU.4) according to [R9].

6.2 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with ALC_DVS.2, ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_TAT.2 and ATE_DPT.3.

7 TOE Summary Specification

7.1 TOE Summary Specification

7.1.1 Chip security functionalities

TSF_DPM

The life cycle of the TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in the TOE as test mode (phase 3) and user mode (phase 4-7). In addition a chip identification mode exists which is active in all phases. The chip identification data (O.Identification) is stored in a in the not changeable configuration page area and non-volatile memory. In the same area further TOE configuration data is stored. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During this first data programming, the TOE is still in the secure environment and in Test Mode. The covered security functional requirement is FAU_SAS.1 "Audit storage". During start-up of the TOE the decision for one of the various operation modes is taken dependent on phase identifiers. The decision of accessing a certain mode is defined as phase entry protection. The phases follow also a defined and protected sequence. The sequence of the phases is protected by means of authentication. The covered security functional requirements are FMT_LIM.1 and FMT_LIM.2. During the production phase (phase 3 and 4) or after the delivery to the customer (phase 5 or phase 6), the TOE provides the possibility to download, after a successful authentication process, a user specific encryption key and user code and data into the empty (erased) Infineon® SOLID FLASH memory area as specified by the associated control information of the Flash Loader software. This process is only possible after a successful authentication process. The integrity of the loaded data is checked with a signature process. The data to be loaded may be transferred optionally in encrypted form. After finishing the load operation, the Flash Loader can be permanently deactivated, so that no further load operation with the Flash Loader is possible. These procedures are defined as phase operation limitation. The covered security functional requirement is FPT_LIM.2 "Limited availability". During operation within a phase the accesses to memories are granted by the MMU controlled access rights and related privilege level. The covered security functional requirements are FDP_ACC.1, FDP_ACF.1 and FMT_MSA.1. In addition, during each start-up of the TOE the address ranges and access rights are initialized by the STS with predefined values. The covered security functional requirement is FMT_MSA.3. The TOE clearly defines access rights and privilege levels in conjunction with the appropriate key management in dependency of the firmware or software to be executed. By this clearly defined management functions are implemented, enforced by the MMU, and the covered security functional requirement is FMT_SMF.1. During the testing phase in production within the secure environment the entire Infineon® SOLID FLASH is deleted. The covered secu-

rity functional requirement is FPT_PHP.3. Each operation phase is protected by means of authentication and encryption. The covered security functional requirements are FDP_ITT.1 and FPT_ITT.1.

TSF_PS

All contents of all memories of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. There is no plain data on the chip. In addition the data transferred over the busses, the SFRs and the peripheral devices (CRC, RNG and Timer) are encrypted as well. The memory content and bus encryption is done by the MED using a complex key management and by the memories Infineon® SOLID FLASH, RAM, CACHE and the bus are entirely encrypted. Note that the FLASH contains the firmware only and no user data. Therefore, no data in plain are handled anywhere on the TOE and thus also the two CPUs compute entirely masked. The symmetric cryptographic co-processor is entirely masked as well. The encryption covers the data processing policy and FDP_IFC.1 ¯Subset information flow control¯. The covered security functional requirements are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1 and FDP_ITT.1. The user can define his own key for an Infineon® SOLID FLASH area to protect his data. This user individually chosen key is then delivered by the operating system and included in the dynamic Infineon® SOLID FLASH encryption. The user specified Infineon® SOLID FLASH area is then encrypted with his key and another component. The encryption of the memories is performed by the memory encryption and decryption unit MED providing protection against cryptographic analysis attacks. The keys which have to be stored on the chip are protected against read out. The covered security functional requirements are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1, and FDP_ITT.1. The CPU has no standard command set and discloses therefore no possibility for deeper analysis. The covered security functional requirement is FPT_PHP.3. The entire design is kept in a non standard way to aggravate attacks using standard analysis methods to an almost not practical condition. A proprietary CPU with a non public bus protocol is implemented, which makes analysis very complicated and time consuming. Important parts of the chip are especially designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA. Therefore, even the physical data gaining is difficult to perform, since timing and current consumption is almost independent of the processed data, protected by a bunch of other protecting means. In the design a number of components are automatically synthesized and mixed up to disguise their physical boarders and to make an analysis more difficult. A further protective design method implements special routing measures against probing. The covered security functional requirements are FPT_PHP.3, FPT_ITT.1 and FDP_ITT.1. In addition to their protection during processing of code and data their storage in the Infineon® SOLID FLASH is protected against side channel attacks too: Even if users operate with direct and static addressing for storing their secrets, the addresses are always translated and modified. In addition the correct privilege level is controlled by the MMU. The covered security functional requirements are FPT_PHP.3, FPT_ITT.1 and FDP_ITT.1. In contrast to the linear virtual address range, the physical Infineon® SOLID FLASH pages are transparently and dynamically scrambled.

These measures cause that the physical location of data is different from chip to chip. Even user software would always call the equal physical addresses. An observation of the clock is used to prevent the TOE from single stepping. This is tested by the user mode security life control UMSLC. The covered security functional requirements are FPT_PHP.3 and FPT_FLS.1. An induced error which can not be corrected will be recognized by the Integrity Guard and leads to an alarm. In case of security critical detections a security alarm and reset is generated. The covered security functional requirement is FPT_FLS.1.

TSF_PMA

First of all we can say that all security mechanisms effective against snooping SF_PS apply also here since a reasonable modification of data is almost impossible on dynamically encrypted, masked, scrambled, transparently relocated, randomized and topologically protected hardware. Due to this the covered security functional requirements are FPT_PHP.3, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1 and FPT_FLS.1. The TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, FLASH and Infineon® SOLID FLASH and includes also the MED, MMU and the bus system. Thus introduced failures are detected and in certain errors are also automatically corrected (FDP_SDI.2). In order to prevent accidental bit faults during production in the FLASH, over the data stored in FLASH an EDC value is calculated (FDP_SDI.1). The covered security functional requirements are FRU_FLT.2, FPT_PHP.3, FDP_SDI.1 and FDP_SDI.2. If a user tears the card resulting in a power off situation during an Infineon® SOLID FLASH programming operation or if other perturbation is applied, no data or content loss occurs and the TOE restarts power on. The Infineon® SOLID FLASH tearing save write functionality covers FPT_FLS.1 "Failure with preservation of secure state" since if the programming was not successful, the old data are still present and valid, which ensures a secure state although a programming failure occurred. This action includes also FDP_SDI.1 "Stored data integrity monitoring" as the new data to be programmed are checked for integrity and correct programming before the page with the old data becomes the new physical page for the next new data. The covered security functional requirement is also FPT_PHP.3 "Resistance to physical attack", since these measures make it difficult to manipulate the write process of the Infineon® SOLID FLASH. The covered security functional requirements are FPT_FLS.1, FPT_PHP.3 and FDP_SDI.1. The TOE is protected against fault and modifying attacks. The core provides the functionality of double-computing and result comparison of all tasks to detect incorrect calculations. The detection of an incorrect calculation is stored and the TOE enters a defined secure state which causes the chip internal reset process. The implementation of two CPUs computing on the same data is by this one of the most important security features of this platform. As the results of both CPUs are compared at the end, a fault induction of modifying attacks would have to be done on both CPUs at the correct place with the correct timing despite all other countermeasures like dynamic masking, encryption and others. As the comparison and the register files are also protected by various measures successful manipulative attacks are seen as being not practical. During start up, the STS performs various configurations and subsystem tests. After the STS

has finished, the operating system or application can call the User Mode Security Life Control (UMSLC) test. The UMSLC checks the alarm lines and number of functions and sensors for correct operation. This test can be released actively by the user software during normal chip operation at any time. In the case that a physical manipulation or a physical probing attack is detected, the processing of the TOE is immediately stopped and the TOE enters a secure state called security reset. The covered security functional requirements are FPT_FLS.1, FPT_PHP.3 and FPT_TST.2. As physical effects or manipulative attacks may also address the program flow of the user software, a watchdog timer and a check point register are implemented. These features allow the user to check the correct processing time and the integrity of the program flow of the user software. Another measure against modifying and perturbation respectively differential fault attacks (DFA) is the implementation of backward calculation in the SCP. By this induced errors are discovered. The covered security functional requirements are FPT_FLS.1, FDP_IFC.1, FPT_ITT.1, FDP_ITT.1 and FPT_PHP.3. The RMS provides the user also the testing of all security features enabled to generate an alarm. This security testing is called user mode security life control (UMSLC). As attempts to modify the security features will be detected from the test, the covered security functional requirement is FPT_TST.2. All communication via the busses is in addition protected by a monitored hardware handshake. If the handshake was not successful an alarm is generated. The covered security functional requirements are FPT_FLS.1 and FPT_PHP.3. The virtual memory system and privilege level model are enforced by the MMU. This controls the access rights throughout the TOE. There is a clear differentiation within the privilege levels defined. The covered security functional requirements are FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMF1.

TSF_PLA

The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of the privileged levels and gives the software the possibility to define different access rights. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges, to a certain extend, for the privilege levels with the exception of the IFX level - is defined from the user software (OS). As the TOE provides support for separation of memory areas the covered security functional requirements are FDP_ACC.1 "Subset access control", FDP_ACF.1 "Security attribute based access control", FMT_MSA.3 "Static attribute initialization", FMT_MSA.1 "Management of security attributes" and FMT_SMF.1 "Specification of Management functions". The TOE provides the possibility to protect the property rights of user code and data by the encryption of the Infineon® SOLID FLASH memory areas with a specific key defined by the user. Due to this key management FDP_ACF.1 is fulfilled. In addition, all memories present on the TOE are individually encrypted using individual keys assigned by complex

key management. All data are protected by means of encryption or masking also during transportation via the busses. Induced errors are recognized by the Integrity Guard concept and lead to an alarm. In case of security critical errors a security alarm is generated and the TOE ends up in a secure state. The covered security functional requirements are FPT_PHP.3, FDP_ITT.1, FDP_IFC.1 and FPT_FLS.1. Beside the access protection and key management, also the use of illegal operation code is detected and will release a security reset.

TSF_CS

The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a co-processor supporting the DES and AES algorithms and a combination of a co-processor and software modules to support RSA cryptography, RSA key generation, ECDSA signature generation and verification, ECDH key agreement and EC public key calculation and public key testing.

7.1.2 Low level security functionalities

TSF_EXECUTION_ENVIRONMENT

This security functionality provides a secure execution environment based on the secure operation of CPU that controls the execution flow, detects and reacts to potential security violations. After start-up, this function calls TSF_BOOT_AT_POWER_UP and waits for a terminal command. This command is either processed or redirected to another item.

In particular, TSF_EXECUTION_ENVIRONMENT manages:

- Application selection
- Applications management (firewall)
- A security group by application (Key status, SECURE MESSAGING status)

Before sending a command to an application, this function tests its (syntaxic) validity. This function initializes a transaction with a previously selected application.

Then, the managed security attributes are:

- when a transaction begins, the allocation of security attribute context and the initialization of all the security group status to (FALSE, FALSE, FALSE)
- when a transaction ends, the release of the security attribute context (memory erasure with TSF_MEMORY_MANAGEMENT)
- the Key status is set to TRUE if mutual authentication has succedeed during phases 4 to 6

the Secure Messaging status is set to TRUE if the current command uses the Secure Messaging, is authenticated and checked for integrity

the Secure Messaging status is set to FALSE after each processed command All the hardware security functionalities are used to produce the secure execution environment.

7.1.3 Operating system security functionalities

TSF_MEMORY_MANAGEMENT

This security functionality manages the persistent and volatile memories of the product according to the capacities of the underlying security IC, so as to control access to sensitive content protected by the TOE. TSF_MEMORY_MANAGEMENT manages the access to objects (files, directories, data and secrets) stored in FLASH. Access for read or write to RAM and FLASH is impossible from the outside, refer to TSF_IO_MANAGEMENT for more information.

An access is granted only if:

The file type is managed by the TOE

The file header is positively checked for integrity

The record that must be accessed is positively checked for integrity

The access conditions are fulfilled TSF_MEMORY_MANAGEMENT manages the erasure of the FLASH and RAM memory. FLASH and RAM erasure are performed by writing random values on it.

Moreover, this security functionality uses TSF_CRYPTO_OPERATION to perform cryptographic operations in order to verify the integrity. CRC (Cyclic Redundancy Check) is the algorithm used to perform integrity tests. This operation concerns file header, file record, OTP zone. All integrity tests link with the Input/Output Buffer is managed by TSF_IO_MANAGEMENT. In phases 4 to 6 of the life cycle, only administration application can perform this access for creating files. Once these files are created, administration applications have all rights on these lasts. The access conditions to files are applied for the phase 7. In phase 7, subjects that can perform access are applications (pre-selected or selected) or the manager. Two access conditions are defined: Check if the concerned file is in the application arborescence. This condition is only used if the application is pre-selected or selected. Application arborescence is composed of all the files under its ADF, of all the elementary files under its DDF and of all the elementary files under its MF (GROUPE ALL). This control ensures the data isolation and applies the inheritance rule for data sharing, Check that the file access attributes are consistent with the operation that must be performed. There exists two attributes for each file, one controls the READ accesses, the other the WRITE accesses. For each attribute, it is precised: The person who can perform the action. The operation can be possible only for a library or an application, for all the applications of an applicative base, or for all the modules of a group, General conditions to the access. These conditions correspond to the security attributes of an application. This test is then performed only in the case where an application is pre-selected or

selected. These conditions are NONE, NEVERand secure messaging (data validity through secure messaging).

The following hardware TSF can be used:

SF_PS Protection against Snooping

SF_PMA Protection against Modification Attacks

SF_DPM Device Phase Management

TSF_BOOT_AT_POWER_UP

This security functionality manages the initialization of the TOE that happens after each reset warm or cold. This security feature performs the following operations:

Test of the following items:

FLASH memory segment

RAM memory

Random Number Generator

Crypto-processor

ATR issuing

Initialization of all modules and applications initialization.

The following hardware TSF are called:

SF_PMA Protection against Modification Attacks

SF_PLA Protection against Logical Attacks

SF_DPM Device Phase Management

TSF_LIFE_CYCLE_MANAGEMENT

This security functionality manages the life cycle of the product and provides a secure transition mechanism between states. The various phases to be recognized are pre-personalization, personalization, usage and end of life. The management of the life cycle is performed by writing information in the One-Time Programmable (OTP) memory. The life cycle of the product is composed of 7 phases, more information is available in the dedicated paragraph 3.2 At the end of the fabrication phase, after a test phase, chip test mode is inhibited in a non-reversible way: the data (system or user) are completely under the control of the card operating system. This is true for read, write or modify operations. Tests done during fabrication phase can not be used anymore.

The following hardware security functionality is used: SF_DPM Device Phase Management, for the management of the OTP memory (user write once)

TSF_CPLC

This security functionality manages the CPLC area. The CPLC area contains Manufacturing data, pre-personalization data and Personalization data. Manufacturing data are written by the Manufacturer during the Manufacturing phase and contain identification data such as founder ID, chip ID and operating system ID. Pre-Personalization data are written by the Manufacturer and also contains identification data such as the module ID. The CPLC area is a write-

only-once area and write access is subject to Manufacturer or Personalization Agent authentication. Read access to the CPLC area is allowed during Personalization phase. During Operational Use phase, the CPLC area read access is only possible after BAC authentication.

TSF_MONITORING

This Security Functionality monitors all the events generated by the security IC physical detectors:

- Bad CPU usage
- integrity loss in FLASH, OTP or RAM,
- code signature alarm,
- fault injection attempt,
- watchdog timeout,
- access attempt to unavailable or reserved memory areas,
- MPU errors,
- clock and voltage supply operating changes by the environment,
- TOE physical integrity abuse.

Executable code integrity is controlled during its execution through the addition of code redundancies and specific tests. Code consistency is then ensured. The following hardware TSF are used:

- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks

TSF_IO_MANAGEMENT

This security functionality manages Input/Output interfaces by way of contact and contactless. Two protocols are used to communicate:

- T=0 protocol, asynchronous, character-oriented half-duplex transmission protocol
- T=CL, specific to the contactless, asynchronous, block-oriented half-duplex transmission protocol

A buffer is used for inputs and outputs. It is a reserved memory zone for the communication. Other memories can not be accessed. During a cryp- tographic operation, the access to this buffer is blocked, once the operation is finished, the integrity of the buffer is verified by a CRC.

The following hardware TSF is used:

- SF_PMA Protection against Modification Attacks

TSF_ALEA

This security functionality provides random numbers. The random number generation is in conformance to the quality requirements of the french national schemes:

- A random number generator compliant with the French Scheme ANSSI requirements for RNG
- A random generator of n bytes.

The chip security functionality is compliant with the AIS31 standard. Conforming to the French Scheme ANSSI requirement for RNG, post-treatment is effectued on the RNG chip output, directly by the chip. The RNG chip output provided by the chip s submitted to a posttreatment in order to provide a random number of n bytes.

7.1.4 Application security functionalities

TSF_KEY_MANAGEMENT

This security functionality provides secure generation, destruction, replacement and storage of cryptographic keys (KEY, …) according to the specification of the product. Each secret is identified by a unique identifier and only manipulated with the help of this identifier by the cryptographic module.

Each secret is associated to a ratification counter. The management of these lasts is made by read/write control of the management of the maximum number of attempts. The ratification counter:

- for a key is initialized to 32 and decremented after each presentation of a wrong MAC,

Keys management consists of the following functions, prior to Issuer authentication, using a random generation of size 8 bytes:

- Loading in the TOE: Keys are protected in integrity and confidentiality during their loading (first loading or update). The cryptographic module ensures their secure storage in the initialization, personalization and user life cycles phases. Loaded keys use is made by the cryptographic module, using the unique key identifier.
- Internal transfer in the TOE: The cryptographic module handles the secure transfer of each key to the cryptographic processor, during its use for a cryptographic identifier.

The following hardware security functionality is used:

- SF_PS Protection against Snooping
- SF_PMA Protection against Modification Attacks

TSF_BAC_AUTH

This security functionality manages the authentication of the Inspection system to the TOE, based on the Document Basic Access Keys. TSF_BAC_AUTH performs the Basic Access Control mechanism, as described in [R9], in order to authenticate the Inspection System. TSF_BAC_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations.

TSF_SYM_AUTH

This security functionality manages the authentication of a user to the TOE, based on the TDES or AES keys related to this user, during the personalization phase. TSF_SYM_AUTH performs an authentication mechanism based on TDES or AES. TSF_SYM_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations.

TSF_CRYPTO_OPERATION

This security functionality performs high level cryptographic operations:

- Encryption/decryption;
- Integrity verification;
- Secret decryption;
- Authentication cryptogram creation/verification;
- Key derivation;
- Hash value calculation.

Encryption/decryption TSF_CRYPTO_OPERATION performs TDES in CBC mode in conformance with FIPS 46-3 [R14] and [R9] normative appendix 5, A5.3 in order to achieve encryption and decryption in secure messaging.

Integrity verification TSF_CRYPTO_OPERATION performs Retail MAC in conformance with ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2), in order to achieve message authentication code in secure messaging.

Secret decryption TSF_CRYPTO_OPERATION performs decryption of ciphered secret imported in the card. This functionality is available in personalization phase only.

Authentication cryptogram creation/verification TSF_CRYPTO_OPERATION performs the following authentication cryptogram calculation/verification:

- Mutual Authentication based on TDES, this mechanism is available in personalization phase only.
- Basic Access Control authentication (see key derivation)
- CBC DES with Retail MAC for secure messaging (see Integrity verification). Authentication cryptogram calculations are performed using a random number in order to avoid replay of the authentication.

Key derivation TSF_CRYPTO_OPERATION performs the Document Basic Access Key Derivation Algorithm to derive Triple-DES and Retail-MAC Session Keys of size 112 bits for secure messaging, from agreed parameters produced during the Basic Access Control Authentication Protocol, as described in [R9] normative appendix 5. Hash value calculation

TSF_CRYPTO_OPERATION performs SHA-1, SHA-224 and SHA-256 **SHA 384 and SHA 512** in conformance with [R16], in order to calculate a hash value.

TSF_ACTIVE_AUTH

This security function manages the capability of the TOE to authenticate itself to the terminal using the Active Authentication Protocol as defined in R9. TSF_ACTIVE_AUTH calls TSF_CRYPTO_OPERATION in order to perform the related cryptographic operations

8 Definitions, Glossary and acronyms

8.1 Acronyms

BIS	Basic Inspection System
CC	Common Criteria
EAL	Evaluation Assurance Level
EFElementary File	
EIS	Extended Inspection System
GIS	General Inspection System
IAS	Identité Authentification Signature
ICAO	International Civil Aviation Organization
ICCSN	Integrated Circuit Card Serial Number
IT	Information Technology
JCRE	Java Card Runtime Environment
JVM	Java Virtual Machine
MF	Master File
MRTD	Machine Readable Travel Document
n.a.	Not applicable
OSP	Organizational security policy
PPProtection Profile	
RAD	Reference Authentication Data
RNG	Random Number Generator
SAR	Security assurance requirements
SDO	Signed Data Object
SFP	Security Function Policy
SFR	Security functional requirement
ST	Security Target
TOE	Target of Evaluation

TSF TOE Security Functions

TSP TOE Security Policy

VAD Verification Authentication Data

VGP Visa Global Platform

8.2 Conventions used

The following list shows the roots used for the various elements.

Root	Elements described by this root
T.	Threats relative to the TOE and the TOE operational environment
OSP.	Organisational security policy
A.	Assumption
OT.	Security objectives for the TOE
OE.	Security objectives for the operational environment

8.3 Definitions

Active Authentication

Security mechanism defined in [5] option by which means the MRTD's chip proves and the inspection system verifies the identity and authenticity of the MRTD's chip as part of a genuine MRTD issued by a known State of Organization.

Application note

Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Audit records

Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.

Authenticity

Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization.

Basic Access Control (BAC)

Security mechanism defined in [R9]] by which means the MRTD's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).

Basic Inspection System (BIS)

An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the MRTD's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical MRTD.

Biographical data (biodata)

The personalized details of the MRTD holder appearing as text in the visual and *machine readable zones* on the biographical data page of a passport book or on a travel card or visa. [R9].

Biometric reference data

Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.

Certificate chain

Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (selfsigned certificate).

Chip

An integrated circuit and its embedded software as it come out of the IC manufacturing step.

Counterfeit

An unauthorized copy or reproduction of a genuine security document made by whatever means. [R9]

Country Signing CA Certificate (CC_{SCA})

Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.

Country Verifying Certification Authority

The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing State or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD.

Current date

The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.

CVCA link Certificate

Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.

Document Basic Access Key Derivation Algorithm

The [R9], normative appendix 5, A5.1 describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.

Document Basic Access Keys

Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key K_{ENC}) and message authentication (key K_{MAC}) of data transmitted between the MRTD's chip and the inspection system [R9]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.

Document Security Object (SOD)

A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [R9]

Document Verifier

Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations.

Eavesdropper

A threat agent with Enhanced-Basic attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.

Enrolment

The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [R9]

Extended Access Control

Security mechanism identified in [R9] by which means the MRTD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data

and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.

Extended Inspection System

A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

Extended Inspection System (EIS)

A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.

Forgery

Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [R9]

General Inspection System

A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.

Global Interoperability

The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [R9]

IC Dedicated Support Software

That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

IC Dedicated Test Software

That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

Initialisation Data

Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).

Inspection

The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [R9]

Inspection system (IS)

A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder.

Integrated circuit (IC)

Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is built on an integrated circuit.

Integrity

Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization.

Issuing Organization

Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [R9]

Issuing State

The Country issuing the MRTD. [R9]

Logical Data Structure (LDS)

The collection of groupings of Data Elements stored in the optional capacity expansion technology [R9]. The capacity expansion technology used is the MRTD's chip.

Logical MRTD

Data of the MRTD holder stored according to the Logical Data Structure [R9] as specified by ICAO on the MRTD's chip. It presents readable data including (but not limited to)

(1) personal data of the MRTD holder

(2) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(3) the digitized portraits (EF.DG2),

(4) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and

(5) the other data according to LDS (EF.DG5 to EF.DG16).

(6) EF.COM and EF.SOD

Logical travel document

Data stored according to the Logical Data Structure as specified by ICAO in the integrated circuit including (but not limited to)

(1) data contained in the machine-readable zone (mandatory),

(2) digitized photographic image (mandatory) and

(3) fingerprint image(s) and/or iris image(s) (optional).

Machine readable travel document (MRTD)

Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [R9]

Machine readable zone (MRZ)

Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [R9]

MRTD application

Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes

- the file structure implementing the LDS [R9]
- the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13 and EF.DG16, EF.COM and EF.SOD) and
- the TSF Data including the definition the authentication data but except
- the authentication data itself.

MRTD Basic Access Control

Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.

MRTD holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

MRTD's Chip

A chip programmed according to the Logical Data Structure as specified by [R9] and ready for personalisation.

MRTD's chip Embedded Software

Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Step 1 and embedded into the MRTD's chip in Step 3 of the TOE life-cycle.

Optional biometric reference data

Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.

Passive authentication

(i) verification of the digital signature of the Document Security Object and

(ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.

Personalization

The process by which the portrait, signature and biographical data are applied to the document. This may also include the optional biometric data collected during the "Enrolment". [R9]

Personalization Agent

The agent acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.

Personalization Agent Authentication Information

TSF data used for authentication proof and verification of the Personalization Agent.

Personalization Agent Authentication Key

Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent.

Physical travel document

Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to)

(1) biographical data,

(2) data of the machine-readable zone,

(3) photographic image and

(4) other data.

Pre-personalization Data

Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Active Authentication Key Pair and the Personalization Agent Key Pair.

Pre-personalized MRTD's chip

MRTD's chip equipped with a unique identifier and a unique asymmetric Active Authentication Key Pair of the chip.

Receiving State

The Country to which the Traveler is applying for entry. [R9]

Reference data

Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.

Secure messaging in encrypted mode

Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4.

Skimming

Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.

Security Target (ST)

Reference document for the TOE evaluation: the certificate awarded by the DCSSI will attest conformity of the product and its documentation with the (functional and assurance) requirements formulated in the security target.

Target of Evaluation (TOE)

The product to be evaluated and its associated documentation.

Terminal Authorization

Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.

TOE Security Functionality (TSF)

A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

Set of rules stipulating how to manage, protect and distribute assets within a TOE.

Travel document

A passport or other official document of identity issued by a State or Organization which may be used by the rightful holder for international travel. [R9]

Traveler

Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.

TSF data

Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [R1]).

Unpersonalized MRTD

The MRTD that contains the MRTD Chip holding only Initialization Data and Pre-personalization Data as delivered to the Personalisation Agent from the Manufacturer.

User data

Data created by and for the user that does not affect the operation of the TSF (CC part 1 [R1]).

Verification

The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [R9]

Verification data

Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

9 Reference and applicable documents

9.1 Reference Documents

Designation	Reference	Title	Revision	Date
Common Criteria				
[R1]	CCMB-2006-09-001	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model	Version 3.1, Revision 4	September 2012
[R2]	CCMB-2007-09-002	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	Version 3.1, Revision 4	September 2012
[R3]	CCMB-2007-09-003	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	Version 3.1, Revision 4	September 2012
[R4]	CCMB-2007-09-004	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology	Version 3.1, Revision 4	September 2012
Protection Profiles and Security Target				
[R5]	BSI-CC-PP-0055	Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application", Basic Access Control	Version 1.10	March 2009
[R6]	BSI-CC-PP-0056	Common Criteria Protection Profile - Machine Readable Travel Document with “ICAO Application", Extended Access Control	Version 1.10	March 2009
[R7]	BSI-PP-0002-2001	Protection Profile, Security IC Platform Protection Profile. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik).	Version 1.0	July 2001
[R8]	BSI-DSZ-CC-0782-2012	Security Target (ST) M7892 B11	Rev 1.1	2012-28-08
E-passport specifications				

Designation	Reference	Title	Revision	Date
[R9]	ICAO Doc 9303	part 1 volume 1, Sixth edition, 2006, Passports with Machine Readable Data Stored in Optical Character Recognition Format; part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability.	Sixth edition	2006
[R10]	TR-03110	Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)	Version 2.10	
CC supporting document				
[R11]	CCDB-2008-04-001	Supporting Document - Mandatory Technical Document - Application of Attack Potential to Smartcards	V2.5, R1	April 2008
[R12]	CCDB-2007-09-001	Supporting Document - Mandatory Technical Document - Composite product evaluation for Smartcards and similar devices	V1.0, R1	September 2007

9.2 Applicable Documents

Designation	Reference	Title	Revision	Date
Cryptography				
[R13]		Technical Guideline :Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI		2006
[R14]	FIPS PUB 46-3	Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standards (DES), U.S. Department Of Commerce / National Institute of Standards and Technology.		Reaffirmed 1999 October 25
[R15]	ANSI X9.31	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998 - Appendix A.2.4		1998
[R16]		Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+ Change Notice to include SHA-224), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology		2002 August 1

Index